INTERSTATE COMMISSION FOR EMS PERSONNEL PRACTICE

Position Paper 2025-01

EMS Workforce Privacy Protection

Adopted by the Commission on February 19, 2025

Introduction

The Interstate Commission for EMS Personnel Practice ("Commission") is committed to the bold protection of all EMS Clinician data. This position paper outlines the critical need to safeguard Personally Identifiable Information (PII) and bulk licensure data of EMS Clinicians, reinforcing the foundational principles of the EMS Compact while calling for consistent standards and practices across all states and State EMS Offices. This effort aligns with federal laws, best practices, and the growing necessity to mitigate risks posed by nefarious actors.

Background

EMS Clinicians play a vital role in protecting public health and safety. The EMS Compact facilitates the cooperation of member states in licensure and regulation, enabling the seamless exchange of information regarding EMS personnel licensure, adverse actions, and significant investigatory details. However, the increasing digitalization of data and the proliferation of cyber threats expose EMS Clinicians to risks such as identity theft, doxxing, and coordinated attacks by malicious actors.

The Commission also recognizes that thousands of EMS Clinicians have primary employment roles beyond EMS, including positions as military personnel, law enforcement officers (local, state, federal), and other federal employees. These dual roles highlight the diverse responsibilities EMS Clinicians undertake, with their licensure being an essential component of their duties. These additional roles are integral to national security preparedness and response efforts. Licensure records for these individuals are often co-located with those of non-military EMS Clinicians. Federal laws, such as the Privacy Act of 1974 and Department of Defense regulations, mandate additional protections for these records, which must be upheld while balancing the need for transparency and public access to essential licensure information.

We recognize the public needs the ability to confirm licensure status of EMS clinicians, this is paramount to consumer protection and transparency. This, however, must be carefully balanced with the need to protect the EMS workforce and emerging national security threats.

The Case for Protecting EMS Clinician Data

The federal government defines PII as protected information. The Commission aligns with this federal definition and considers the following EMS Clinician data as PII, which should be strongly protected , and generally not released, as part of public records requests:

- Social Security number (SSN), passport number, driver's license number, taxpayer identification number .
- Personal address, personal email addresses, and personal phone number.

- Biometric records such as photographic images (especially of face or other distinguishing characteristics), fingerprints, retina scans, voice signatures, and facial geometry.
- Bulk information that, when combined with other request details, can easily identify specific EMS Clinicians. Examples may include: date of birth, place of birth, race, religion, geographical indicators, employment information, or education information.

Misuse of PII can lead to:

- Financial loss, identity theft, and harassment for individuals.
- Reputational damage, legal liability, and administrative burdens for organizations.

In the context of EMS Clinicians, excessive release of bulk data, including detailed PII, exposes them to heightened risks such as doxxing and coordinated large-scale attacks by terrorists or adversaries. Such scenarios are unacceptable and underscore the need for robust data protection measures.

Recommendations

To address these challenges, the Commission calls upon all State EMS Offices, including EMS Compact Member States and non-member states, to adopt the following measures:

1. Vigilance Against Nefarious Intent:
    - Be vigilant when responding to requests for bulk data to identify potential malicious intents.
    - Seek assistance from the Department of Justice (DOJ) and FBI to vet any foreign actors or their agents requesting bulk data.
2. Protection of PII:
    - Ensure PII is not disclosed improperly.
    - Prevent the unauthorized release of military or federal agency affiliation for EMS Clinicians with such affiliations. All bulk data must adhere to federal privacy protection requirements.
3. Standardization of Public Portals:
    - Create consistent public portal standards to validate EMS Clinician licensure and EMS Compact Privilege to Practice (PTP) status.
    - Allow searches by:
        - First and last name.
        - State issued EMS license number.
        - National EMS ID number.
    - Prohibit Boolean wildcard searches (e.g., First Name: A*, Last Name: S*) and bulk data disclosures.
    - Restrict the public display of information to the following:
        1. First and last legal name on record.

2. State/jurisdiction of licensure.
3. License level.
4. License expiration date.
5. License status (e.g., active, expired, restricted, revoked).
6. Final agency action information, if applicable, available and authorized.

4. Alignment with Federal Standards:
    - Recognize the federal definition of PII as protected information and adhere to its associated safeguards.
    - Implement privacy protections aligned with the Privacy Act of 1974, ensuring data is collected, maintained, and disclosed responsibly.

Position

Therefore, it is the position of the Commission that all states should take action to protect EMS Clinicians' data while ensuring the public's ability to validate licensure and authorization to practice.

- States must thoroughly validate that all data requests are not originating from foreign sources, or agents of foreign sources.
- States should ensure robust procedures are in place to confirm the legitimacy of data requestors.
- States must prohibit the release of Personally Identifiable Information (PII) as part of public records requests.
- States should ensure all military and federal employee EMS licensure data are handled in compliance with federal laws and regulations.
- States must establish standard protections and review processes for all bulk data requests, ensuring alignment with federal guidelines and best practices.
- States should review state laws to ensure EMS Clinicians have the same data privacy protection afforded to law enforcement, public health, and elected officials.

By implementing these recommendations, states can maintain a critical balance between transparency and security, safeguarding the personal and professional well-being of EMS Clinicians. This approach not only fulfills the purposes of the EMS Compact but also addresses the evolving challenges of data security in a digital age.